# DoH and DoT Server Discovery

## & Deployment Considerations for Home and Mobile Networks

M. Boucadair (Orange)
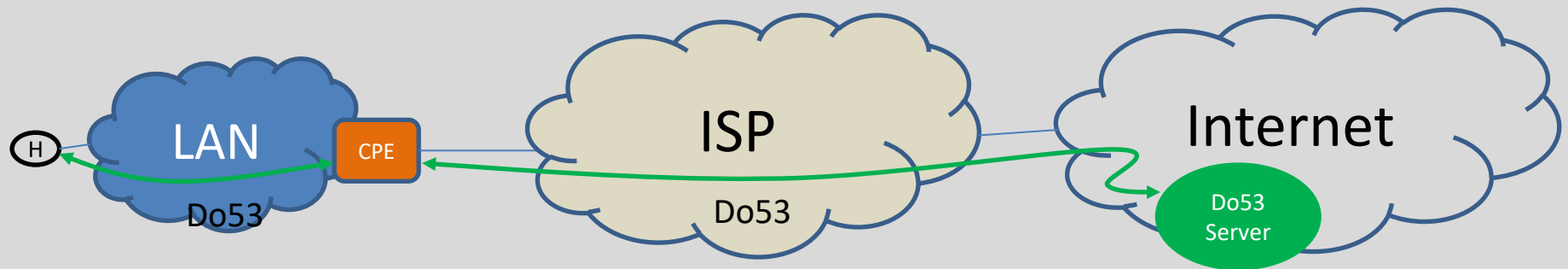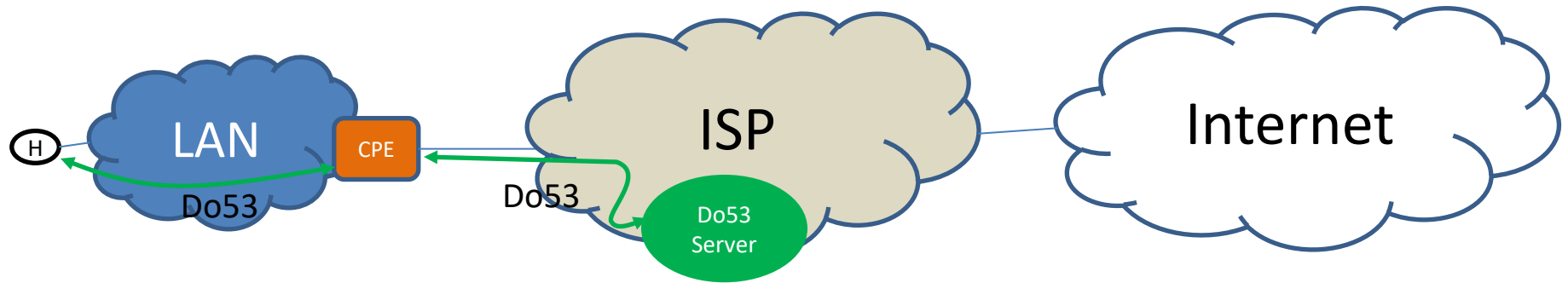T. Reddy (McAfee)
D. Wing (Citrix)
N. Cook (Open-Xchange)

# Agenda

- Scope & Objectives
- Target DoT/DoH deployments
- Which discovery information?
- The discovery procedure
- Rogue servers
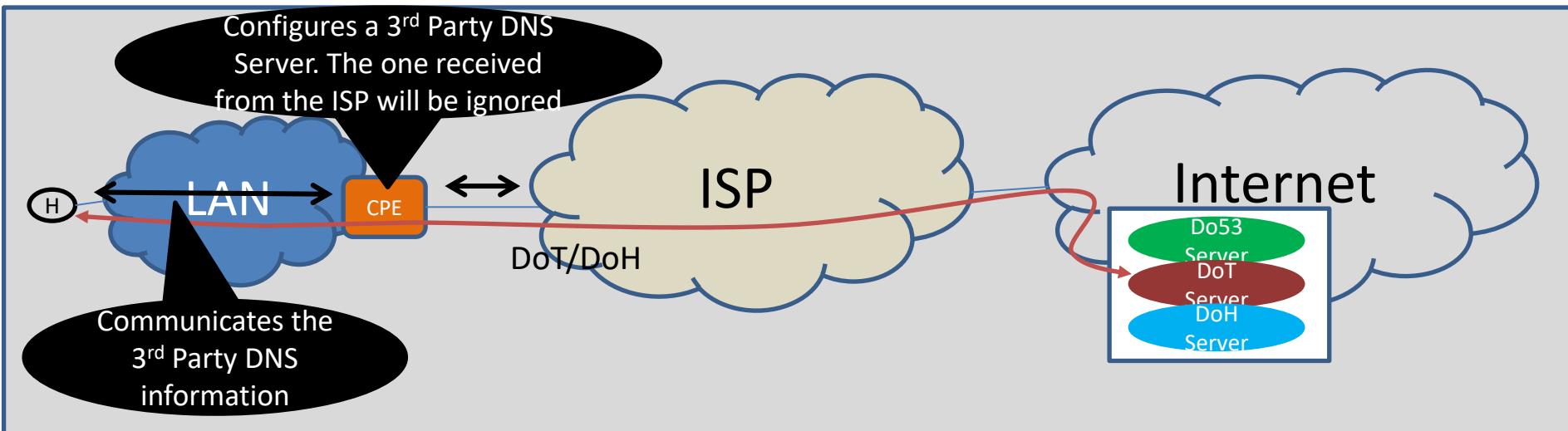- DoH-specific: one pending issue
- Next steps

# Objectives
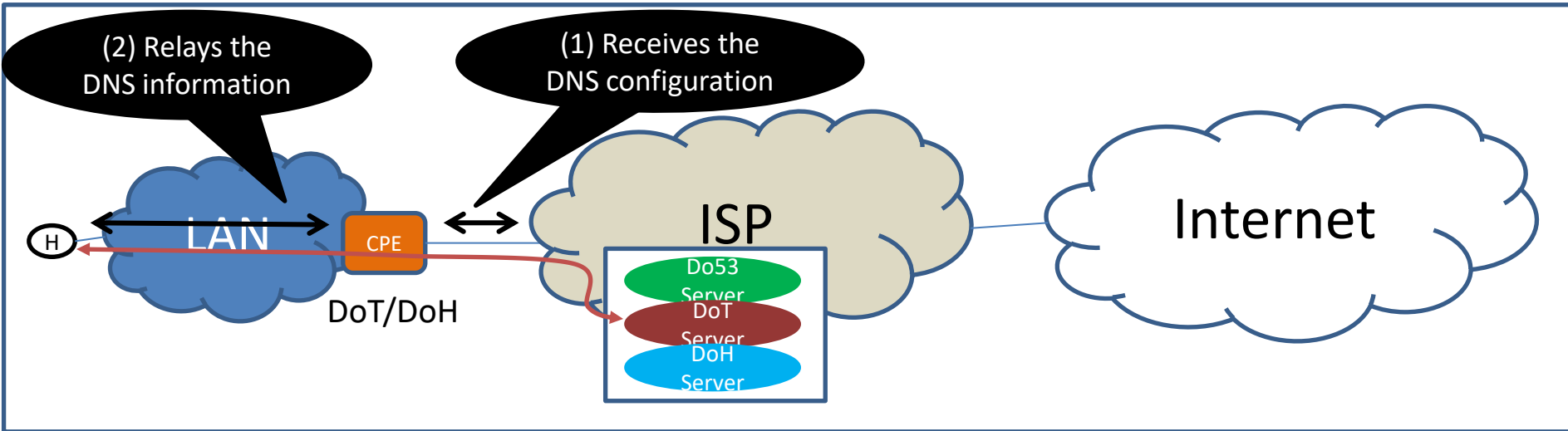
- Discuss DoT/DoH deployment considerations for **home networks**
  - Both Home and Mobile networks
  - ISP, public, and private resolvers

- Specify the required **server discovery mechanism(s)**

- Sketch the **required steps** to use DoT/DoH capabilities provided by local networks

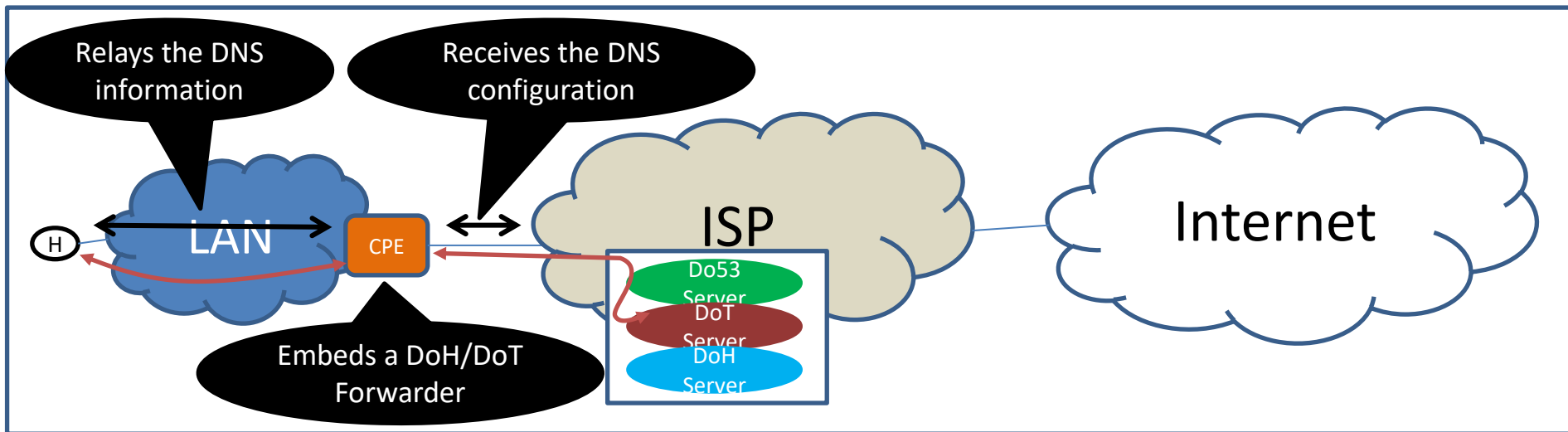# Sample Legacy Deployments

# Sample Encrypted DNS Deployments: Managed CPEs



DoT/DoH: Means DoT and/or DoH

# Sample Encrypted DNS Deployments: Managed CPEs (2)



Relays the DNS information

Receives the DNS configuration

LAN

H

CPE

Embeds a DoH/DoT Forwarder

ISP

Do53 Server

DoT Server

DoH Server

Internet

# Sample Encrypted DNS Deployments: Unmanaged CPEs
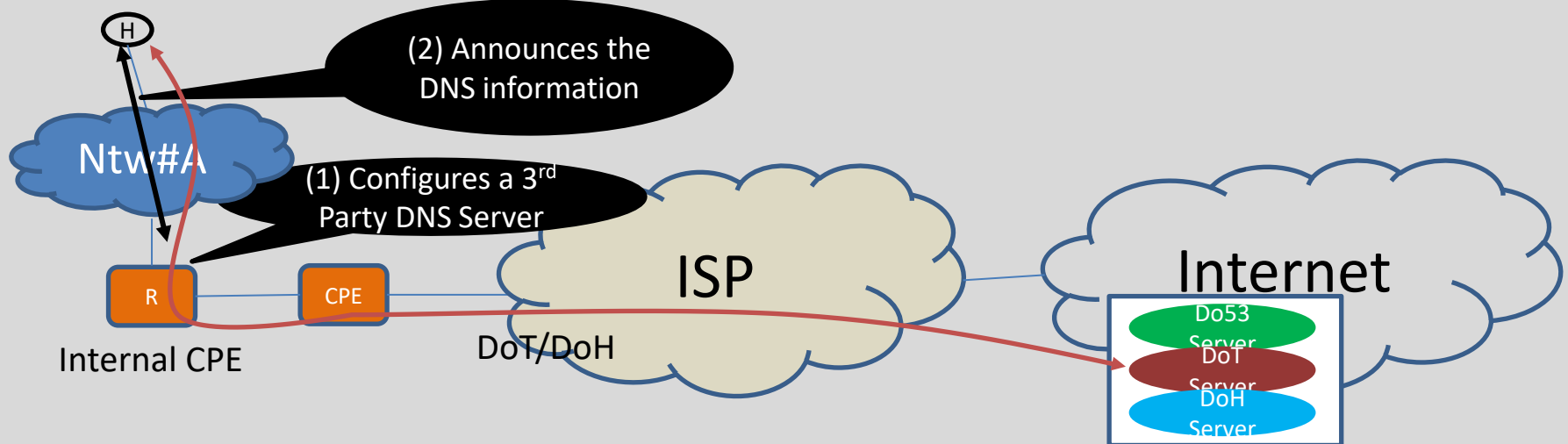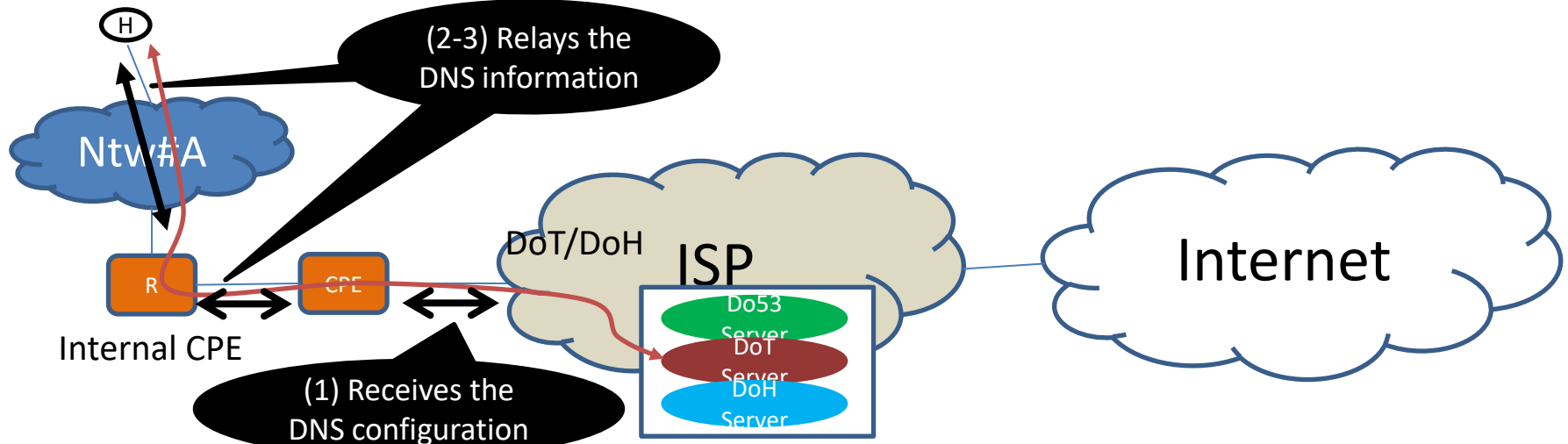
# Which Discovery Information is Needed?

| Do53 | DoT | DoH |
|------|-----|-----|

List of IP addresses

Authentication Domain Name

URI Templates

To avoid relying upon Do53 or opportunistic profile to resolve the resolver's name

For PKIX authentication

1. Other URI variables
2. DoH resolvers may expose customized services: no-filtering, filtering+malware detect, filtering+adult block, …
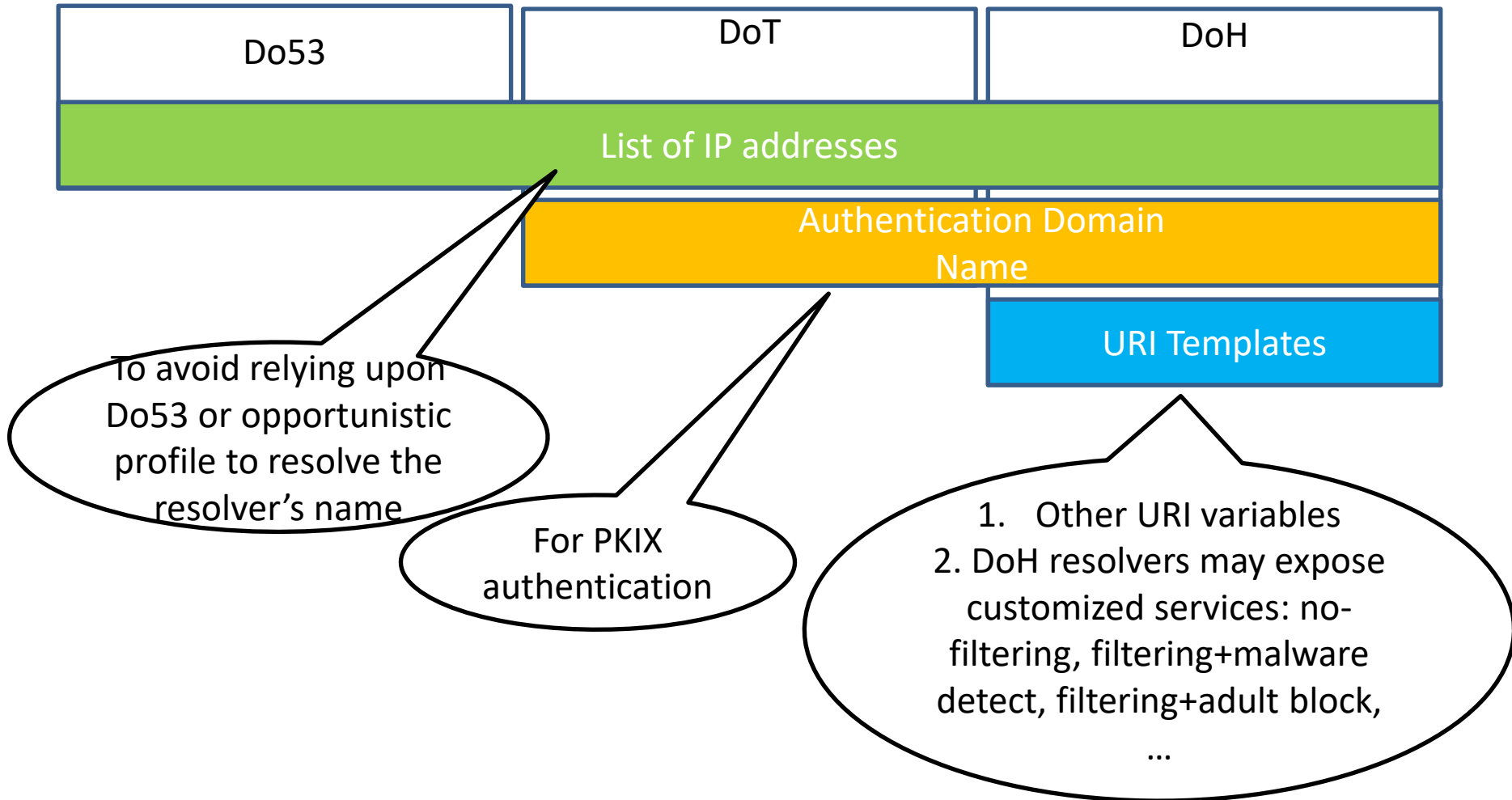
# Which Channel for Discovery?

| Do53 | DoT | DoH |
|------|-----|-----|

**List of IP addresses**

**Authentication Domain Name**

**URI Templates**

Leverage existing DHCP/RA/PCO options

Define a new DHCP/RA/PCO option: Reference Identifier

Retrieved directly from the DoH server or using a dedicated RA/DHCP/PCO option
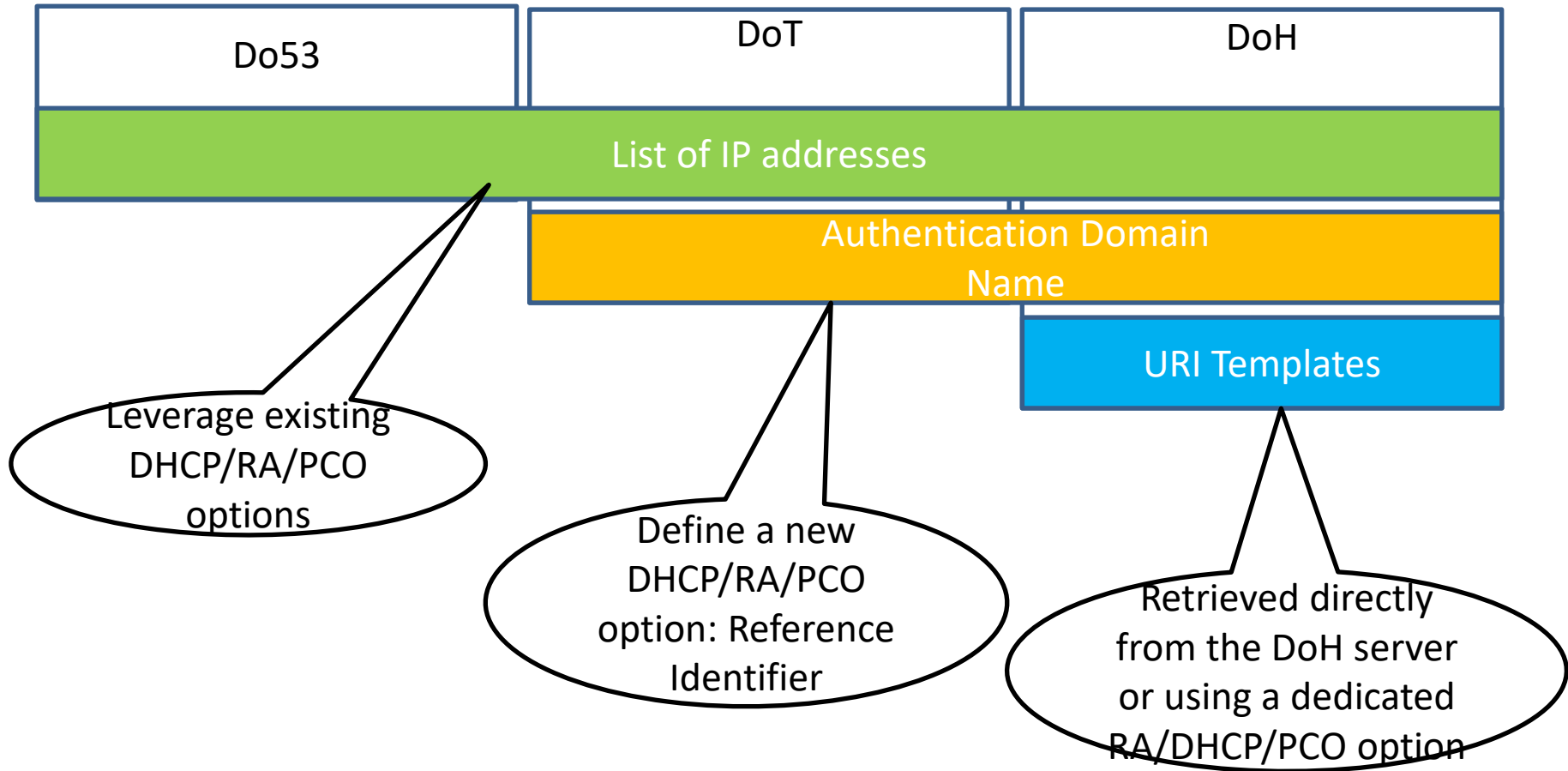
# What about Rogue Servers?



Speech bubble text:
(1) Gets a valid name and a valid certificate
(2) Announces that name in an DHCP/RA RI option

Labels in diagram: H, RA(A), Ntw# A, A, CPE, ISP, Do53 Server, DoT Server, DoH Server, Internet, S, Attack Server
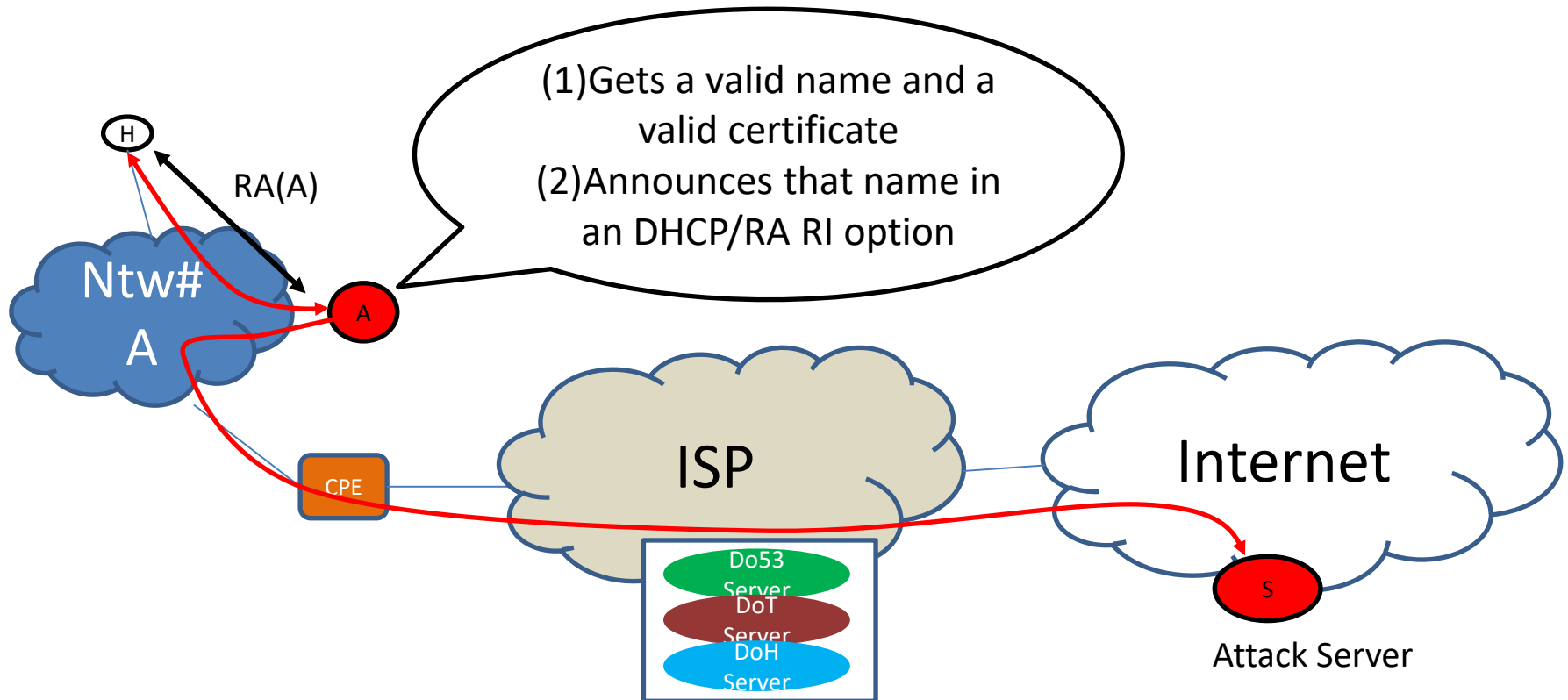
# Rogue Servers Will be detected

DNS servers conveyed in RA/DHCP messages from rogue servers **won't be used** by the host because the address(es)/ADN is not pre-configured in the OS or browser as a **verified resolver**
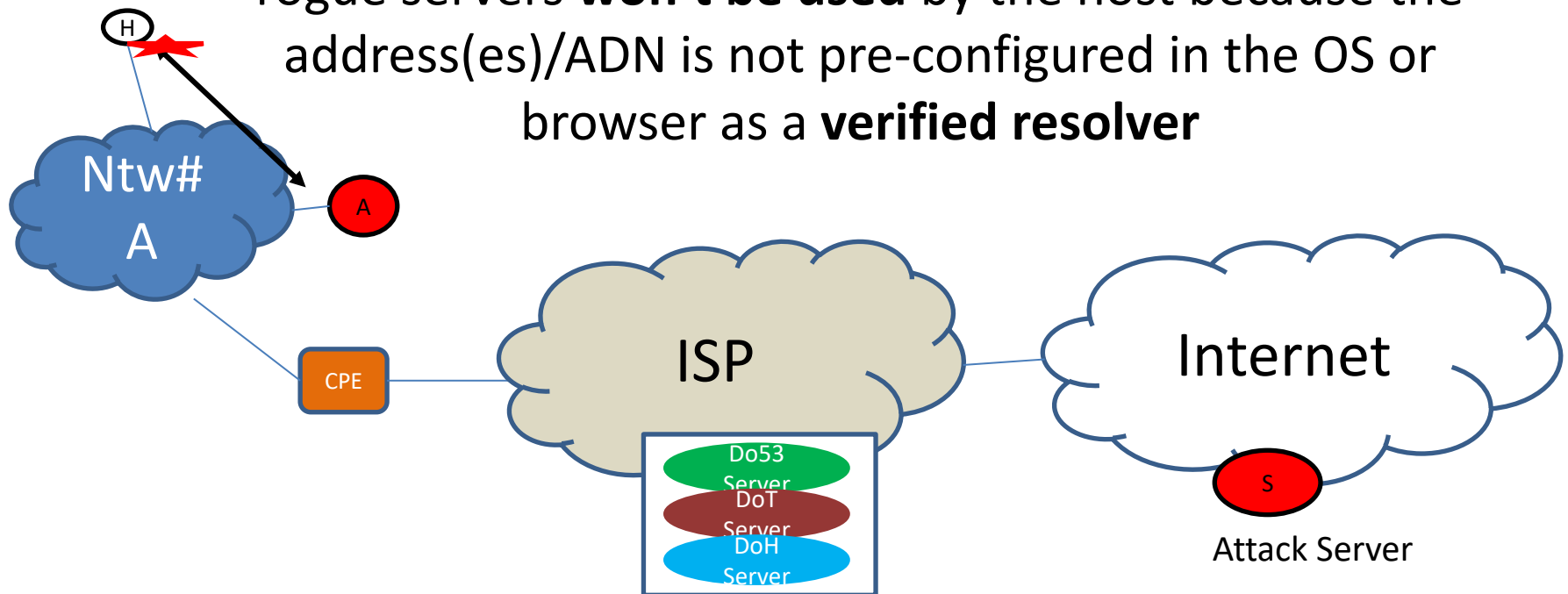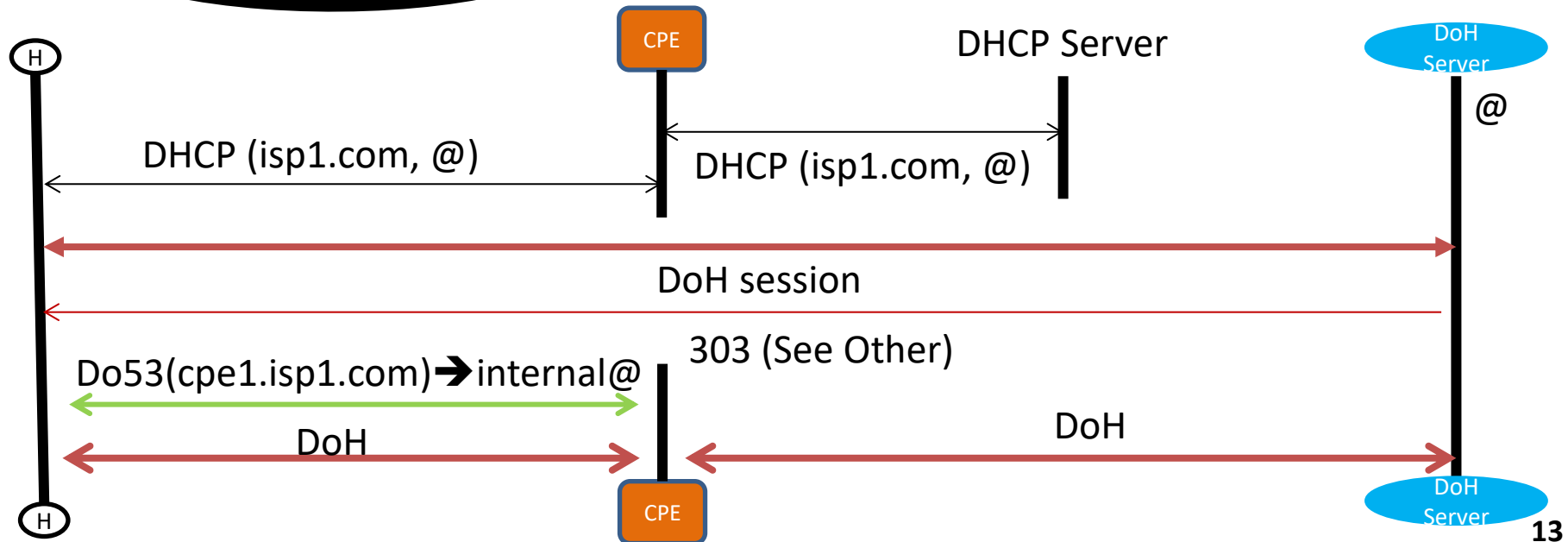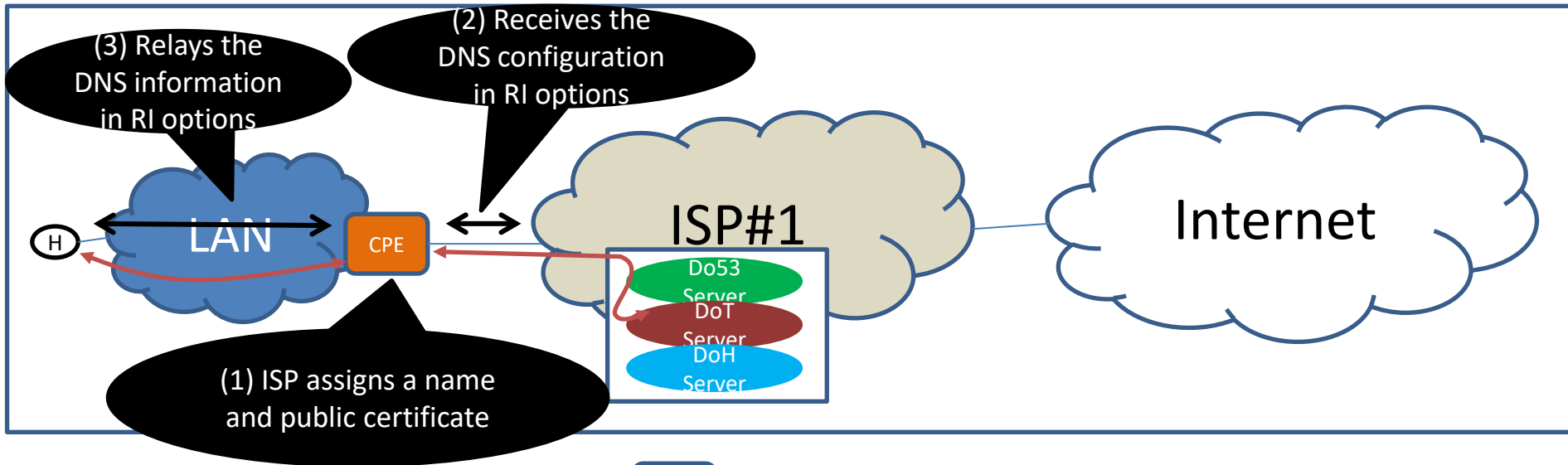


Ntw# A

H

A

CPE

ISP

Do53 Server

DoT Server

DoH Server

Internet

S

Attack Server

# Verified Resolvers

- Auto-upgrade
  - If the **DNS server's IP address** discovered using DHCP/RA is pre-configured in the OS or Browser as a verified resolver, the DNS client auto-upgrades to use the pre-configured DoH/DoT server tied to the discovered DNS server IP address

  - If the **ADN** conveyed in DHCP/RA is pre-configured in the OS or browser as a verified resolver, the DNS client auto-upgrades to establish a DoH/DoT session with the ADN

- Other approaches are discussed in the draft, e.g.,
  - If the discovered DoH/DoT server is not pre-configured in the OS or browser, the client may validate the signatory (e.g., cryptographically attested by the ISP)

# Host a Forwarder in a Managed CPE

(3) Relays the DNS information in RI options

(2) Receives the DNS configuration in RI options

LAN

H

CPE

ISP#1

Do53 Server

DoT Server

DoH Server

Internet

(1) ISP assigns a name and public certificate

H

CPE

DHCP Server

DoH Server

@

DHCP (isp1.com, @)

DHCP (isp1.com, @)

DoH session

303 (See Other)

Do53(cpe1.isp1.com)➜internal@

DoH

DoH

H

CPE

DoH Server

**13**

# Do53 for Redirect: **Not a** Threat

# Host a Forwarder in a Managed CPE

(3) Relays the DNS information in RI options

(2) Receives the DNS configuration in RI options

LAN

H

CPE

ISP#1

Do53 Server

DoT Server

DoH Server

Internet
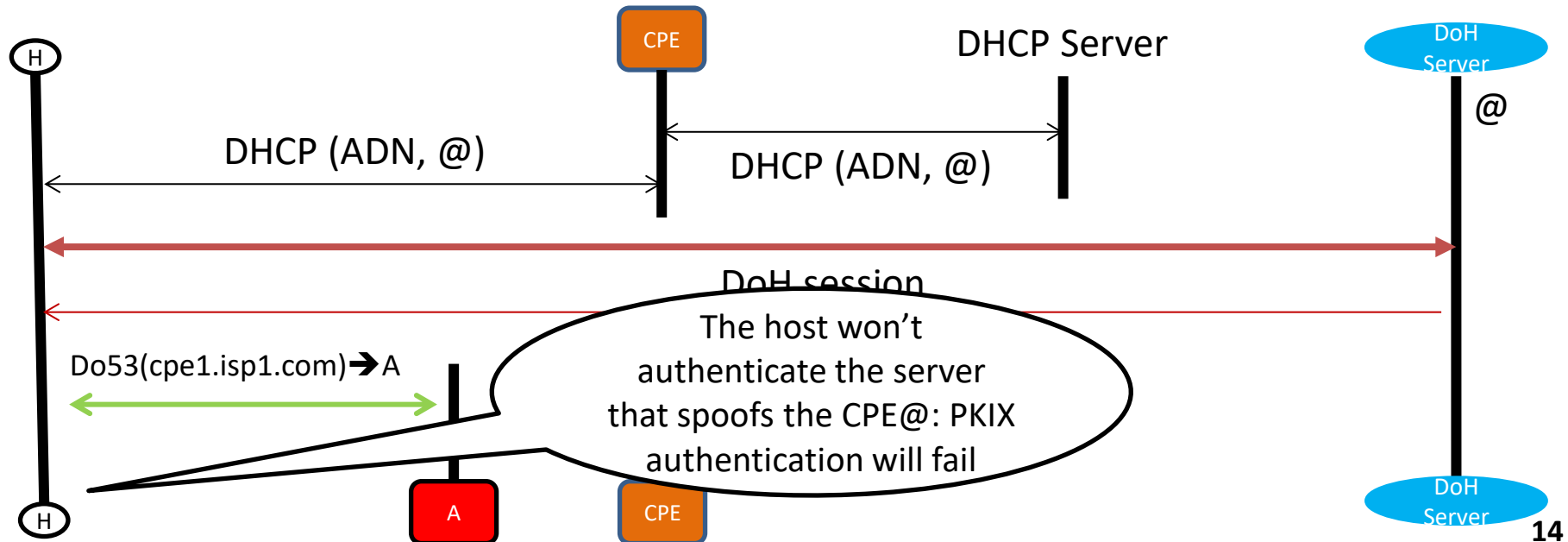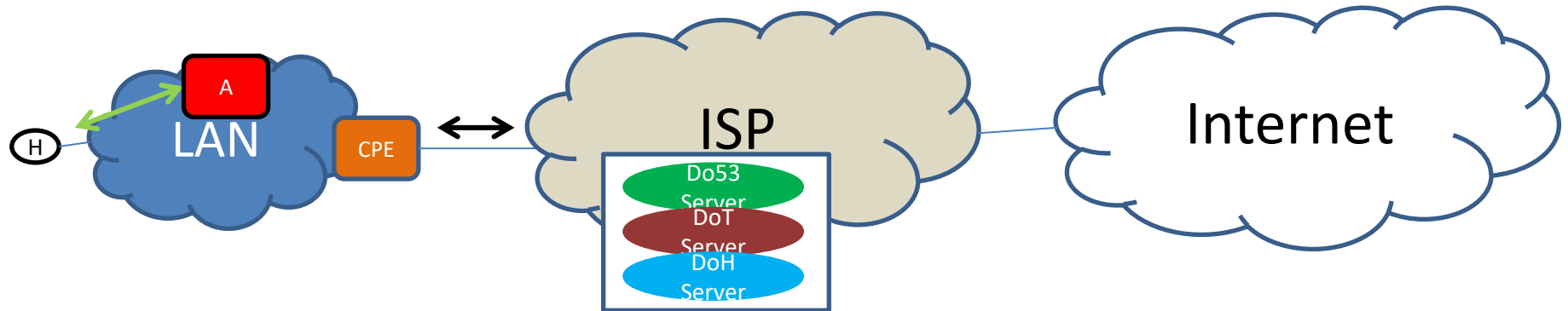
(1) ISP assigns a name and public certificate
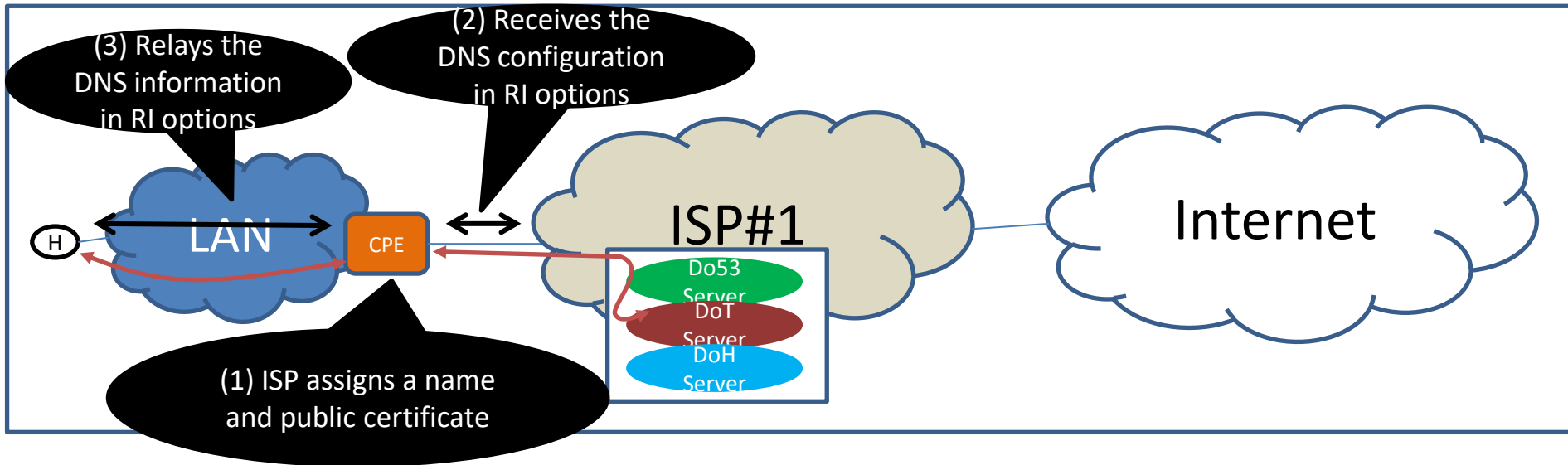
- Certificates are managed by the **ISP**
- ACME fully automates certificate management (e.g., certificate issuance, expiry etc.) and **no human intervention is required**
- ACME and https://letsencrypt.org/ (to generate certificates for millions of home routers) are already in place by some security vendors. No roadblocks is reported so far.
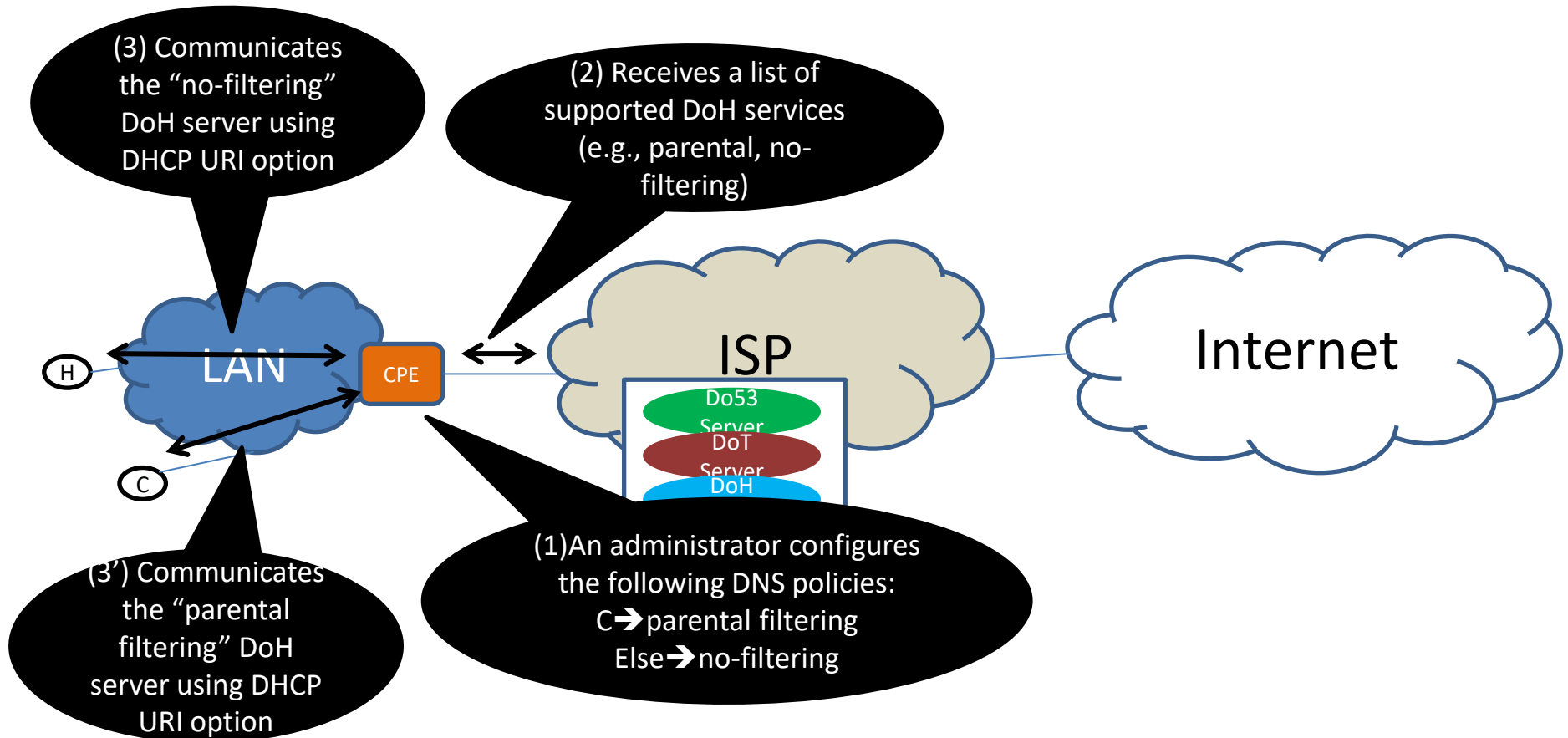
# DoH Services & URI Templates

- Why?
  - RFC8484 supports URI templates with "dns" as the only variable, but future extensions may allow for queries with **other variables**
  - DoH resolvers may host **many services**; each identified by a URI scheme
  - DoH clients have to be instructed about **valid URI templates** to use

- How?
  - retrieved by querying a discovered DoH resolver
  - enclosed in a dedicated RA/DHCP option

- How the client uses these services is out of scope

Pending Issue

# URI Templates in RA/DHCP?

- Trade-offs are discussed in the document:
  - Some Issues
    - Risk of stale information
    - Create a dependency between DHCP servers (access routers) and DoH resolvers
    - Need for an out of band mechanism if the DoH resolver is not managed by the ISP
    - May increase the size of RA/DHCP messages
  - Some advantages
    - Clients can immediately use the service(s)
    - Convenient if very few (stable) URIs are in use
    - Customized (local) configuration
- Do we need to pick one?
  - If yes, which one?

Pending Issue

# Customized DHCP Configuration: An Example



(3) Communicates the "no-filtering" DoH server using DHCP URI option

(2) Receives a list of supported DoH services (e.g., parental, no-filtering)

(3') Communicates the "parental filtering" DoH server using DHCP URI option

(1)An administrator configures the following DNS policies:
C→parental filtering
Else→no-filtering

LAN

CPE

ISP

Internet

Do53 Server

DoT Server

DoH

H

C

Pending Issue

# Implementation

- Ported DNSDist v1.4.0 with DoT/DoH support to OpenWRT-19.07

- Extended DNSDist to do DoT/DoH in the upstream (CPE to resolver)